NETC-G-0412-002-E-STD

NETCOM Technical Authority (TA) Implementation Memorandum For

Army End-User Computing Environment

Version 2.0
19 June 2012

Note: This document supersedes all versions of TA 2003-005.

This document is not to be distributed or changed without express permission from the Network Enterprise Technology Command (NETCOM). This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom of Information Act (FOIA). Exemption 5 applies (internal advice, recommendations, and subjective evaluations that are reflected in records pertaining to the decision-making process of or among agencies).

Distribution

This document is intended for use by US Government agencies and their Contractors doing business with the U.S. Army Network Enterprise Technology Command. This document is for information purposes only and is not to be construed as directive in nature or official policy. This document is available by request from NETCOM, ATTN: NETC-G, 2133 Cushing Street, Fort Huachuca, AZ 85613-7070

THIS PAGE IS INTENTIONALLY BLANK

DISCLAIMER

The contents of this document are not to be construed as an official Department of the Army position unless so designated by other authorized documents. The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to:

NETCOM G5
ATTN: NETC-G
Fort Huachuca, AZ 85613-7070

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

BOMBA.MICHAEL.DENNIS.1132575548 Digitally signed by BOMBA.MICHAEL.DENNIS.1132575548 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=BOMBA.MICHAEL.DENNIS.1132575548 Date: 2012.06.19 06:30:06 -07'00'

19-Jun-2012

MICHAEL D. BOMBA
Director PP&A
ACofS, G5

DATE

MATCHETTE.DANIEL.ROBERT.1041419128 Digitally signed by MATCHETTE.DANIEL.ROBERT.1041419128 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=MATCHETTE.DANIEL.ROBERT.1041419128 Date: 2012.07.02 18:23:56 -07'00'

02-Jul-2012

DANIEL R. MATCHETTE
COL USA
ACofS, G5

DATE

DOCUMENT REVISION LIST

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete re-issue of entire document.

Date	Description of Changes	Organization
21 Dec 2011 9 Sep 2011 Mar-Apr 2012	Added: Information Assurance section. Added: Virtual Desktop Infrastructure section Updated entire document to reference current standards in all related areas.	G5/ESB

TABLE OF CONTENTS

1.0 INTRODUCTION 1
2.0 SCOPE 1
2.1 DEFINITIONS 1
2.2 ACRONYMS 2
3.0 REFERENCES 2
4.0 BACKGROUND 2
5.0 GUIDANCE 2
5.1 MICROSOFT WINDOWS BASELINE 2
5.2 APPLE CONFIGURATION BASELINE 7
5.3 VIRTUAL DESKTOP INFRASTRUCTURE (VDI) 8
5.4 ENERGY EFFICIENCY REQUIREMENTS 9
6.0 RESOURCE IMPACT 10
6.1 LIFE CYCLE UPGRADES 10
6.2 KEYBOARD, VIDEO AND MOUSE (KVM) SWITCHES 10
APPENDIX A: ACRONYMS AND DEFINITIONS A-1
APPENDIX B: REFERENCES B-1

LIST OF TABLES

TABLE 1 MS WINDOWS RECOMMENDED HARDWARE CONFIGURATIONS 4
TABLE 2 CURRENT SOFTWARE PRODUCTS LIST 5
TABLE 3 RECOMMENDED THIN/ZERO CLIENT HARDWARE 9

EXECUTIVE SUMMARY

This Technical Authority (TA) identifies the recommended hardware, operating systems, applications, and configurations necessary to establish a secure, standardized baseline end-user computing environment for use throughout the Army. End-user computing environments documented in this TA include Microsoft Windows and Apple OS X used in desktop, mobile and virtual computing environments.

1.0 Introduction

This TA specifies hardware, operating systems, software and configurations necessary to establish the Army secure, standardized common end-user computing environment. The end-user computing system baselines established within this TA are defined as LandWarNet (LWN) Configuration Items (CIs) and will be managed under the LWN Change Management (CM) process controlled by the LWN Change Control Board (CCB). Submit requests for changes to the established baseline CIs via e-mail to netcom.hq.lwnccb@mail.mil for approval determination.

2.0 Scope

This TA applies to all Army Activities, including Active Army, Army Reserve, and Army National Guard and is mandatory for all Army operated common end-user computing environments on both the Non-secure Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet). This TA is not mandatory for PM managed special purpose computing environments. PMs wishing to use the baselines established by this TA should meet the minimum hardware, software and configuration of system components established by this document.

2.1 Definitions

2.1.1 Common end-user computing environments include zero/thin client, workstation, laptop, tablet, slate and virtual desktop infrastructure solutions. A computing environment, for the purpose of this document, consists of:

a. Hardware
b. Operating System
c. Software applications
d. Configuration settings

2.1.2 DoD Unified Master Gold Disk (UMGD) is a DoD CIO managed initiative to consolidate and standardize Service specific (e.g. AGM) efforts and deliver a single DoD-wide operating system, baseline applications and configuration. The purpose of the UMGD is to enable a secure, standardized common end-user computing environment across DoD. The Army is working to merge the AGM effort into the UMGD effort and for the purpose of this TA, AGM and UMGD shall be considered the same and will be used interchangeably.

2.1.3 Army Golden Master (AGM) is an Army managed program to distribute enterprise licensed operating systems (OS), applications and the necessary configurations to meet United States Government Configuration Baseline (USGCB) guidance and aligns with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). The AGM program supports no more than two versions of any operating system. Currently the supported baselines are Windows 7 and Windows Vista. The AGM/UMGD standard baseline configurations also include common applications listed in Table 2. The AGM/UMGD operating systems baselines are licensed as an upgrade to existing licensed Windows operating systems. The AGM/UMGD baseline is provided to PM Computer Hardware Enterprise Software and Solutions (CHESS) commodity buy PC vendors and is shipped as a part of new end-user computing devices purchased through this vehicle. Use of

the AGM/UMGD is mandatory and any deviation must be approved as per instructions in paragraph 5.1.3.

2.1.4 Zero/Thin client refers to both zero and thin virtual desktop client devices. Zero client refers to devices that do not include an embedded operating system and are used to connect to a virtual desktop infrastructure solution. Thin client refers to devices that include an embedded operating system and are used to connect to a virtual desktop infrastructure. Both zero and thin clients lack local data storage and have strong port controls to determine if printing or other USB connected services are allowed or restricted.

2.1.5 VDI refers to the Virtual Desktop Infrastructure. The Army refers to this as the Virtual End user Environment (VEUE). This environment includes backend servers and storage required to support thin, zero, and mobile client devices.

2.2 Acronyms

Refer to Appendix A for a complete list of acronyms and their definitions.

3.0 References

Refer to Appendix B for a complete list of references.

4.0 Background

DoD has established the goal for end-user computing to “Go Anywhere, Connect and Be Productive”. This goal allows any authorized user, using any authorized device to connect to any authorized network, authenticate and connect to any authorized service or capability. DoD has also established the Joint Information Environment (JIE) effort to streamline, standardize, secure, and make more efficient the delivery of networked services to all DoD users. To achieve these objectives, the Army and DoD have recognized the need to standardize the common end-user computing environment and under the UMGD program, from which these standards will be applied DoD-wide. This TA supports the DoD and Army initiatives by establishing minimum baseline configurations within the Army common end-user computing environment based on AGM and emerging UMGD specifications.

5.0 Guidance

5.1 Microsoft Windows Baseline

5.1.1 Hardware. Systems purchased must be capable of running 32 and 64 bit versions of the current AGM/UMGD. Slate form factor is currently exempt from the requirement to run the 64bit version of the AGM/UMGD. The current minimum hardware recommendations in Table 1 are for planning hardware purchases to accommodate current and future releases of Microsoft Windows OS:

MICROSOFT WINDOWS RECOMMENDED HARDWARE CONFIGURATION	**Workstation**	**Desktop**	**Laptop**	**Lightweight/ Tablet/Slate**
Audio Support	UAA, AAC, or Intel High Definition Audio	UAA, AAC, or Intel High Definition Audio	UAA, AAC, or Intel High Definition Audio	UAA, AAC, or Intel High Definition Audio
Card Reader*	CCID Compliant	CCID Compliant	CCID Compliant	CCID Compliant
Hard Drive**				
SATA Disk Drive	300GB	300GB	N/A**	64GB (self encrypting drives required when available)
Self Encrypting SATA Disk Drive**	256GB	256GB	160GB	64GB
Self Encrypting SATA Solid State Drive (SSD) **	160GB	160GB	160GB	64GB
Input Devices	Section 508 1194.26 compliant 2-button W/ Scroll Wheel	Section 508 1194.26 compliant 2-button W/ Scroll Wheel	Touchpad or stylus capable	Touchpad or stylus capable
Memory	4GB (w/1 free memory)	4GB (w/1 free memory slot)	4GB (w/1 free memory slot)	2GB
Network Support				
Ethernet NIC	802.3u – 10/100/1000 BASE-TX	802.3u – 10/100/1000 BASE-TX	802.3u – 10/100BASE-TX	(optional)
Wi-FI NIC	N/A	N/A	802.11 b/g/n 802.11i WPA2 Enterprise Certified Wi-Fi Alliance Certified	802.11 b/g/n 802.11i WPA2 Enterprise Certified Wi-Fi Alliance Certified
Peripheral Support				
USB 2.0 External Ports	6 free USB (2.0 version) ***	4 free USB (2.0 version) ***	2 free USB (2.0 version) ***	1 free USB (2.0 version) ***
USB 3.0 External Ports	Optional ***	Optional ***	Optional ***	Optional ***
Processor	Minimum 2Ghz Quad Core	Minimum 2Ghz Dual Core	Minimum 2GHz Dual Core	Minimum 1 Ghz Dual Core

EPEAT	Bronze	Bronze	Bronze	N/A
EPA Energy Star	V5.0 or higher	V5.0 or higher	V5.0 or higher	N/A
Removable Media	4X DVD+-DL RW 16X DVD 24X CD	4X DVD+-DL RW 16X DVD 24X CD	4X DVD+-DL RW 8X DVD 24X CD	4X DVD+-DL RW 8X DVD 24X CD External Drive
Video Support	Dual independent view capable	Dual independent view capable	Dual independent view capable	Direct X 10 compatible
System BIOS ****	NIST SP800-147 Compliant (Tamper Resistant)	NIST SP800-147 Compliant (Tamper Resistant)	NIST SP800-147 Compliant (Tamper Resistant)	NIST SP800-147 Compliant (Tamper Resistant)
UEFI BIOS				
Trusted Platform Module (TPM) *****	TCG TPM V1.2 with Core Root of Trust Measurements	TCG TPM V1.2 with Core Root of Trust Measurements	TCG TPM V1.2 with Core Root of Trust Measurements	TCG TPM V1.2 with Core Root of Trust Measurements

Table 1 Recommended Hardware Configurations for Microsoft Windows

* Common Access Card readers must meet the CCID standard and be on the Microsoft Hardware Compatibility List for the current AGM/UGM version at the time of purchase.

** Due to the internal design of SSD, software wipe utilities are ineffective. All SSD purchased will support hardware encryption using the OPAL standard. All Self Encrypting Drives will require setting and escrowing of a recovery password as well as setting of a user password. All new mobile devices will be purchased with Self Encrypting Drives (disk or SSD).

*** At least one USB port must support boot from USB device (e.g. external CD/DVD, external storage).

**** Tamper resistant BIOS (NIST SP800-147) is required on all workstation, laptop and lightweight form factor systems and highly desired on all tablets and slates.

***** As a part of any new purchase, TPM functionality will be turned on and enabled. This will allow Army to take ownership and enable core services like Microsoft BitLocker or machine identity without requiring touch labor.

5.1.2 Software. The current minimum software requirements for the Windows based end-user computing environment are documented in Table 2. Some of these products are currently enterprise licensed and incorporated within the AGM/UGM distribution disks. Other products are not yet covered by the UGM but are still required as a part of future end-user computing device purchases.

Functional Area	Product
Operating System	Microsoft Windows 7 Enterprise 32 and 64bit (AGM supported)
Web Browser	Internet Explorer - (AGM supported)
Office Productivity Suite (includes: Access, Excel, Outlook, PowerPoint, Word, and Publisher)	Microsoft Office Professional (AGM supported)
PDF Viewer	Adobe Acrobat Reader X (AGM supported)
Visio Document Viewer	Microsoft Visio Viewer (AGM supported)
Antivirus Software (Select one of the options)	Symantec Anti-Virus client (AGM supported) McAfee Anti-Virus client (AGM supported)
Form Management	IBM Lotus Forms Viewer (AGM supported) Salinas ApprovIT - (AGM supported)
Smart Card	ActivIdentity ActivClient (AGM supported)
Compression Utility	Native to the OS
Media Player	Microsoft Media Player (AGM supported)
System Management	Microsoft System Center Configuration Manager (SCCM) client agent - (AGM supported)
Online Certificate Status Protocol (OCSP)	Tumbleweed Desktop Validator (AGM supported)
JAVA Runtime Environment	SUN JAVA Runtime Environment (J2SE) (AGM supported)
TPM and SED Management	Software to manage TPM and Self Encrypting Drive passwords (Provided by vendor)
Driver Package	Provided by vendor in a format easily used for automated image deployment using SCCM

Table 2 Current Software Products list

5.1.3 Compliance. The AGM/UMGD will be loaded on all end-user computing devices. Non-compliant systems will require an Army Cyber Command approved Plan of Actions and Milestones (POA&M) identifying how and when the system will be brought into compliance. Army Cyber Command will oversee a LWN Waiver and Governance process that adjudicates deviations from the above specifications by vetting DAA-approved POA&Ms through appropriate risk assessment and governance boards.

5.1.4 General Information

TPM is a secure crypto-processor computer chip (microcontroller) usually installed on the motherboard of a computer designed to provide basic security-related functions that can securely store artifacts used to authenticate the platform (Personal Computer (PC) or laptop). The TPM is also used to store platform measurements that help ensure the platform remains trustworthy. Microsoft further uses the TPM as one of the factors necessary to manage their full disk encryption solution called BitLocker Drive Encryption (BDE). TPM's need to be turned on and enabled in the machine's BIOS. This is a requirement for all purchases and will eliminate the need for touch labor when using the TPM to perform functions outlined in this TA.

Full disk encryption is required on all devices. Full disk encryption can be implemented using hardware based self-encrypting drives or software solutions like Microsoft's BDE. When utilizing BDE, devices in a non-physically secure environment, TPM plus PIN is required for authentication. In physically secured environments, the use of TPM is required, but the use of a PIN is optional. When a drive protected by BDE is removed from a computer, it cannot be decrypted unless the recovery password is provided. The AGM program settings ensure that BDE cannot be enabled until the recovery password is securely stored in Active Directory. Common attack vectors mitigated by using the above guidance include theft of a device (e.g. laptop) or inadvertent disclosure as a result of replacement of a desktop or mobile device drive.

Trusted Computing Group specifies behavior of boot processes with TPM enabled systems to include a Trusted Boot process. Commercially this is an emerging capability that ensures the BIOS and operating system has not been tampered with. This is accomplished by the use of the TPM to measure the BIOS and critical operating system files before these files are allowed to execute. If a change is identified, the trusted boot process stops the file from executing and notifies the user. When combined with appropriate management systems, these notifications are captured as IA events. While the Army does not currently implement Trusted Boot, it is an emerging capability the Army plans to leverage once it is commercially viable.

Tamper Resistant BIOS prevents unauthorized modifications of firmware in accordance with NIST SP800-147. This policy applies to all U.S. Army organizations and all procurement specifications for IT hardware (personal computer client systems including desktops and laptops), software and services. The CHESS office will host the instructions that will assist Army end users and Network Enterprise Centers (NECs) in identifying platforms that are compliant with NIST SP800-147 standard (current offerings, planned support, and update of legacy platforms) as well as steps necessary to update legacy platforms. (https://chess.army.mil/ascp/commerce/index.jsp).

802.1x provides an open standards solution to authenticating a computer's access to the network. It is supported by all major networking equipment manufacturers and is an integrated component in all Army approved operating systems. The use of 802.1x requires machine identity be verified as a part of the connection to the network process. To ensure this process supports all of DoD as well as Army travelers, the token used to identify the machine identity needs to be independent of the Active Directory forest the machine is a member of. DoD PKI non-person entity (NPE) certificates will be used within the Extensible Authentication Protocol Transport Level Security (EAP-TLS) standard for this purpose. The TPM will be used to adequately protect these NPE certificates, the TPM will be used. The basis for the standards associated with this process is in the Trusted Computing Group's Trusted Network Connect specification.

Trusted Network Connect specification as defined by the Trusted Computing Group provides more than machine identity for port based authentication. This standard also provides for PC Health Checks that can be utilized to make decisions on what logical network (VLAN) the machine connects to. The goal of this specification is to ensure machines with known problems are not allowed on production LAN segments. This is an emerging capability and once commercially viable, will be implemented by DoD.

5.2 Apple Configuration Baseline

5.2.1 Hardware Baseline. A specific hardware baseline is not provided for Apple systems as the vendor (Apple) ships only an integrated (hardware and operating system) product and certifies the hardware to work with the operating system.

5.2.2 Software Baseline. Apple does not ship an AGM/UMGD baseline for their computers. It is therefore necessary to update the baseline as necessary to meet current STIG or USGCB requirements and process appropriate requests to NETCOM for approval of a Certificate of Networthiness prior to placing these systems on DoD networks. For systems capable of running OS X 10.6.8, the AGM program has packaged a release that meets these standards and is pre-approved (Certificate of Networthiness) for use on Army networks. The AGM Apple configuration baseline documentation is available from the AGM homepage at: https://www.us.army.mil/suite/page/130061.

5.2.3 Compliance. The AGM/UMGD will be loaded on all end-user computing devices. Non-compliant systems will require an Army Cyber Command approved Plan Of Actions and Milestones (POA&M) identifying how and when the system will be brought into compliance. Army Cyber Command will oversee a LWN Waiver and Governance process that adjudicates deviations from the above specifications by vetting DAA-approved POA&Ms through appropriate risk assessment and governance boards.

5.2.4 General Information

The Apple product release model is “computer-specific" to hardware coupled with the most current Operating System. Computer-specific versions of Apple OS X include special software that lets the OS work seamlessly with the new model's hardware, and is required for the computer to work correctly. Apple will not certify or support earlier versions of the Apple OS X operating systems on newer versions of Apple hardware. (i.e. Apple Snow Leopard which was released in 2009 may not operate on newer Apple Hardware released in fall 2011.)

In order for current AGM Apple OS X 10.6.8 systems to join Active Directory (AD) environments that have been smart card login enabled (e.g. Common Access Card (CAC) Cryptographic Login), a third party AD client software package is required.

Current Apple file/folder encryption solutions (e.g. filevault) will not work with a CAC and is not currently FIPS certified. DoD policy requires encryption of data at rest on all mobile devices. To comply with this mandate will require acquisition and integration of a FIPS compliant Data at Rest (DAR) solution on all Apple mobile (e.g. laptop) devices.

Some Windows programs such as MS Project and MS Visio are not Apple OS compatible. Non-compatible programs are available via virtual machine software within the Windows OS.

5.3 Virtual Desktop Infrastructure (VDI)

The Army is pursuing efforts to establish and implement an Army VDI standard in order to virtualize desktop computing environments. Where appropriate, the VDI will be used to support business and operational mission requirements and gain long term IT cost benefits by delivering more effective and efficient IT services, desktop standardization and improved IT security. The VDI must support delivery of the Army's standard desktop as a service to non vender specific client hardware being used as the user's desktop. Additionally, the VDI must support different front-end hardware configurations including but not limited to: Zero Clients, Thin Clients, Mobile Clients, and Thick Clients.

Considerations for the implementation of VDI include:

a. AGM baseline support
b. Support CAC or SIPRNet PKI Token (Smart Card:
c. Authentication to DoD networks
d. Signing and Encryption of email
e. Authentication to PKI enabled websites and applications (e.g. DoD Enterprise Email)
f. Digital signatures on documents

5.3.1 VDI Client Devices

Zero/thin client devices do not typically have a dedicated local hard drive. In a VDI, all client device applications and user data are stored on the servers where all significant processing is also performed. All zero/thin client platforms being considered will be compliant with the current Army regulations and STIGs for use on the LWN Enterprise.

VDI implementations require strong port access control mechanisms that deny all port access (e.g. USB devices) and selectively allow peripherals such as scanners, printers, storage, etc. Most virtual client devices fall into one of the following categories:

Zero clients: These are stateless clients with no embedded OS that typically use protocols such as PC over Ethernet (PCoE) to communicate with back end virtual desktop solutions.

Thin clients: These are stateless clients with an embedded OS (e.g. Windows Embedded). Thin Client OS images are typically managed by special software and management tools provided by the thin client manufacturer.

Diskless workstations: These are typically legacy user workstations with the disk removed using boot over LAN technologies such as pxe boot to load a memory resident OS. Use of diskless workstations should be discouraged and only used as a bridging solution to either zero or thin clients.

Virtual client: These are zero or thin clients emulators that operate on user workstations, notebooks, tablets, slates or smart phones. Virtual clients will be addressed in future releases of this TA.

Table 3 shows the recommended hardware specifications for zero and thin clients.

5.3.2 VDI Backend Systems. Zero/thin client back end solutions will be addressed in a future TA specific to zero/thin client solutions.

RECOMMENDED HARDWARE CONFIGURATION	Thin Client	Zero Client
Audio Support	UAA, AAC, or Intel High Definition Audio**	UAA, AAC, or Intel High Definition Audio**
Card Reader*	CCID Compliant	CCID Compliant
Input Devices	Section 508 1194.26 compliant (1) 2-button W/ Scroll Wheel (1) 104 Key Keyboard	Section 508 1194.26 compliant (1) 2-button W/ Scroll Wheel (1) 104 Key Keyboard
Memory	2GB RAM	NA
Network Support	RJ-45 Gigabit Ethernet 10/100/1000	RJ-45 Gigabit Ethernet 10/100/1000
Peripheral Support	(4) USB (2.0) (1) audio headphone output jack (1) Microphone input audio jack	(4) USB (2.0) (1) audio headphone output jack (1) Microphone input audio jack
Processor	1 GHz	N/A
EPEAT	Bronze	Bronze
EPA Energy Star	V5.0 or higher	V5.0 or higher
Video Support	Dual independent view capable	Dual independent view capable

Table 3 Recommended Thin/Zero Client Hardware

* Common Access Card readers must meet the CCID standard and be on the Microsoft Hardware Compatibility List for the current AGM/UGM version at the time of purchase..

5.4 Energy efficiency requirements

IAW AR25-1, and Executive Order (EO) 13123, all new purchases of desktop and notebook/laptop equipment will meet Environmental Protection Agency (EPA) energy star requirements for energy efficiency. Additionally, all applicable desktops, workstations, and devices will be configured as directed by Army Cyber Command power management policies.

a. **Computers:** After 30 minutes of inactivity, computers—desktops and laptops—will enter into hibernate mode. The Power Options for the Army Golden Master will be set to put the computer to sleep in 30 minutes and a Group Policy will be used to push this requirement out to ensure consistency.

b. **Monitors**: After 15 minutes of inactivity, monitors and laptop displays will enter into sleep mode. The Power Options for the AGM will be set to put the monitor/display to sleep in 5 minutes and a Group Policy will be used to push this requirement out to ensure consistency.

c. **Other Peripheral Equipment:** After 30 minutes of inactivity, other peripherals such as printers, scanners, facsimiles, all-in-one devices, and copiers, will enter into sleep mode. When setting up new equipment, the NEC needs to set the appropriate sleep mode before putting the equipment in service. For existing equipment, NEC personnel should update the equipment by setting the sleep mode for the designated time.

6.0 Resource Impact

6.1 Life Cycle Upgrades

Hardware lifecycle replacement is the responsibility of the owning (user) organization. IAW AR-25-1 paragraph 6–2. Computing Services, organizations will use Product Manager CHESS, to the maximum extent possible, to purchase COTS software, desktops, and notebook computers regardless of dollar value and for all other IT purchases greater than $25K. If a requirement cannot be satisfied based on this criterion against a CHESS contract, a waiver may be granted. Requests for waivers will be submitted through the CHESS Web site at https://chess.army.mil

6.2 Keyboard, Video and Mouse (KVM) Switches

DoD maintains a mandatory approved products list for KVM devices used to share peripherals across unclassified and classified networks. This list can be found at https://aplits.disa.mil/processAPList.do.

Appendix A: Acronyms and Definitions

Acronyms	Definition
AAC	Advanced Audio Coding
ACOM	Army Command
AD	Active Directory
ADCS	Active Directory Certificate Services
ADDS	Active Directory Domain Services
AGM	Army Golden Master
AKA	Also Known As
AKO	Army Knowledge Online
AR	Army Regulation
ASCC	Army Service Component Command
BIOS	Basic Input / Output System
CA	Certificate Authority
CAC	Common Access Card
CARE	Customer Access and Reporting Environment
CCB	Change Control Board
CCRM	Change Configuration Release Management
CHESS	Computer Hardware Enterprise Software and Solutions
CI	Configuration Item
CM	Change Management
CNDSP	Computer Network Defense Service Provider
CPU	Central Processing Unit
DAA	Designated Approving Authority
DAR	Data At Rest
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DoD	Department of Defense
DRU	Direct Reporting Unit
DTS	Defense travel System
DVD	Digital Video Disc
DVI	Digital Visual Interface
ELA	Enterprise License Agreement
EO	Executive Order
EPA	Environmental Protection Agency
EPEAT	Electronic Product Environmental Assessment Tool
ESD	Electronic Software Delivery
ESB	Enterprise Services Branch
FDCC	Federal Desktop Core Configuration
FTP	File Transfer Protocol

GB	Gigabyte
GHz	Gigahertz
HW	Hardware
IAM	Information Assurance Managers
IAPM	Information Assurance Program Managers
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IDE	Integrated Drive Electronics
IEEE	Institute of Electrical and Electronics Engineers
IM	Information Management
INE	In-line Network Encryptor
KCC	Knowledge Collaboration Center
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LWN	LandWarNet
LWN(C)	LandWarNet (Classified)
LWN(U)	LandWarNet (Unclassified)
MAC	Macintosh
MS	Microsoft
NA	Network Administrator
NAP	Network Access Protection
NEC	Network Enterprise Center
NETCOM	Network Enterprise Technology Command
NIPRNet	Non-Secure Internet Protocol Router Network
NPE	Non-Person Entity
O&M	Operation & Maintenance
OS	Operating System
PC	Personal Computer
PCR	Platform Configuration Register
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan Of Action & Milestones
POC	Point of Contact
PP&A	Plans, Programs & Architecture
RCIO	Regional Chief Information Officer
RDS	Remote Desktop Services
SA	System Administrator
SANS	SysAdmin, Audit, Network, Security
SATA	Serial Advanced Technology Attachment

SCCM	System Center Configuration Manager
SIPRNet	Secure Internet Protocol Router Network
Slate	As defined in Energy Star computer specification version 5.0
SRK	Storage Root Key
SRR	Security Readiness Review
SPAN	Sharing Peripherals Across the Network
SRK	Storage Root Key
STIG	Security Technical Implementation Guides
SW	Software
TA	Technical Authority
TCG	Trusted Computing Group
TPM	Trusted Platform Module
UAA	Universal Audio Architecture
UMGD	Unified Master Gold Disc
VDI	Virtual Desktop Infrastructure
VEUE	Virtual End User Environment
VPN	Virtual Private Network
WDDM	Windows Display Driver Model
WSUS	Windows Server Update Services

Appendix B: References

a. Army Regulation (AR) 25-1, Army Knowledge Management and Information Technology Management, 4 December 2008

b. Army Regulation (AR) 25-2, Information Management, Information Assurance, 23 March 2009

c. DRAFT Army Regulation (AR) 25-2, Army Information Management Information Assurance, 12 October 2011.

d. Memorandum, CIO/G-6, Subject: Army Thin Client Computing Guidance, 15 November 2010,

e. Secretary of the Army Guidance for Information Technology Management Reforms, 9 September 2011

f. DoD Directive 8000.1, Global Information Grid (GIG) Overarching Policy, 10 February 2009

g. DoD Directive 8500.1, Information Assurance, 24 October 2002

h. DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003

i. DoD Regulation O-8530.01-M, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program, 17 December 2003

j. DoD Regulation 8570.01-M, Information Assurance Workforce Improvement Program, Change 2, 20 April 2010, 19 December 2005

k. DISA General Desktop Application STIG, Version 4, Release 1, 03 December 2009

l. Memorandum, SAIS-IOM" Army Policy for use of the Army's Microsoft Enterprise License Agreement (ELA), 4 February 2004.

m. Defense Information Systems Agency (DISA), Sharing Peripherals across the Network (SPAN) Keyboard Video Mouse (KVM), Version 2, Release 1, Security Technical Implementation Guide (STIG), dated 29 April 11.

n. DISA General Desktop Application STIG, Version 4, Release 1, 03 December 2009

o. Operation Order 0910-300, Data At Rest (DAR) Deployment, Appendix 1 (BitLocker / EFS TTP), 24 February 2010.

p. Trusted Computing Group - Trusted Platform Module. TPM is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (PC or laptop).

q. DoD Memorandum – Policy for DAR/TPM Encryption of Sensitive Unclassified Data At Rest on Mobile Computing Devices and Removable Storage Media, DoD, July 3, 2007

r. MS TechNet Library - Changes in TPM Management - Applies To: Windows 7, Windows Server 2008 R2. TPM Management is a Microsoft Management Console (MMC) snap-in that allows administrators to interact with TPM Services. TPM Services is used to administer the TPM security hardware computer laptop and desktops. Updated: May 18, 2009

s. MS TechNet Library - Using Smart Cards with BitLocker Applies To: Windows 7, Windows Server 2008 R2. In Windows 7, smart card certificates can be used with BitLocker Drive Encryption to protect fixed and removable data drives and to recover BitLocker-protected drives in the absence of the *primary access key. Updated: November 11, 2009.*

t. MS TechNet Library - TPM Management - Applies To: Windows 7, Windows Server 2008 R2. TPM Management is a Microsoft Management Console (MMC) snap-in that allows administrators to interact with TPM Services. TPM Services is used to administer the TPM security hardware in your computer.

u. MS TechNet Library - Changes in TPM Management - Applies To: Windows 7, Windows Server 2008 R2. TPM Services is used to administer the TPM security hardware in your computer. In Windows 7 and Windows Server 2008 R2, the TPM Management snap-in now can be used to reset the TPM lockout value. Updated: May 18, 2009.

v. MS TechNet Library - Network Access Protection (NAP) is a feature in Windows Server 2008 that controls access to network resources based on a client computer's identity and compliance with corporate governance policy. Updated April 21, 2011

w. MS TechNet Library - NAP and TPM integration development of new standards of integrating the TPM into solutions like NAP. May 21, 2007

x. MS TechNet Library - BitLocker Group Policy Reference - Applies To: Windows 7, Windows Server 2008 R2. Updated: May 3, 2010

y. MS TechNet Library - Store TPM Recovery information in Active Directory Domain Services - Applies To: Windows 7, Windows Server 2008 R2. Active Directory Domain Services (AD DS) can be used to store TPM recovery information.

z. MS TechNet Library - Group Policy control of TPM - Applies To: Windows 7, Windows Server 2008 R2. Using Group Policy to control TPM commands.

aa. MS TechNet Library - Backing Up BitLocker and TPM Recovery Information to Active Directory. BitLocker and TPM recovery information can be backed up in Active Directory. A package containing the actual keys used to encrypt the data as well as the recovery password required to access those keys. Updated: June 21, 2008.

bb. Cisco - SSL VPN Security (IPSEC and TPM) Host Identity Verification

cc. DISA - The Non-Person Entity (NPE) Initiative IPSec tunnels using device certificates. Cyber, Identity and Information Assurance (CIIA). Use of TPM in NPE. Fall 2011, Volume 2, Issue 3.

dd. DISA - Network Infrastructure - Network Access Control, Version 8, Release 1, Supplement of Network Infrastructure STIG, V8R1. NAC is a suite of collective technologies that provide three functions for the DoD. These three functions of access control consist of Device Authentication, Device Policy Assessment, and Device Policy Remediation. March 24, 2010.

ee. BIOS Protection Guidelines, Special Publication 800-147, April 2011

ff. PC Client Specific Trusted Platform Module TPM Family 1.2; Level 2 Revision 116, Version: 1.2; Trusted Computer Group 2003-2011